IP Lock [IPL-010L/030L]取扱い説明書 [Ver1.7]

はじめに

この度はAES暗号処理方式・IPセキュリティシステム「IP Lock ラボラトリーズパック[IPL-010L/030L]」をご採用頂き誠にありがとうございます。本IPL-010L/030L（以下、IP Lockとします)は、信頼性の極めて高いAES暗号処理技術を採用したFPGAロジックセキュリティです。IP LockコアをFPGAに組み込み、暗号処理コントローラチップ(以下、暗号処理チップ)と接続するだけで、お客様の重要なFPGA内のIP資産をプロテクトします。

本ラボラトリーズパックでは、ユーザ専用の ID が付属の暗号処理チップにあらかじめ書き込まれておりますので、チップをボードに実装し IP Lock コアを FPGA にインプリメントするだけですぐにご使用いただけます。ユーザ専用IDは各ラボラトリーズパックのセットごとに異なったユニークなIDとなっており、本IDを持った暗号処理チップは本パックの他に存在致しません。

パッケージ内容

IP Lockのパッケージ内容は下記のとおりです。

- 暗号処理チップ（IPL-010Lは10個、IPL-030Lは30個）
- CD-ROM
  - Altera社製FPGA用IP Lockコア（TopIPLock.vhd, iplock.vhd）
  - Xilinx社製FPGA用IP Lockコア（TopIPLock.vhd, iplock.ngc , iplockex.ngo）
  - VHDLデザイン例ソースコード（Counter.vhd, Counter32Bits.vhd）
  - IP Lock取扱説明書（IPL-MAN-V1.xJ.pdf、本ファイル）

使用上の注意事項

IP Lockの使用時は以下の注意事項を厳守してください。

[1] 本ラボラトリーズパックでは、デザイン・ゲートウェイにより出荷時にユーザ専用のIDが暗号処理チップにあらかじめ書き込まれておりますので、IDをお客様が変更することはできません。

[2] ユーザ専用のIDは各ラボラトリーズパックのセットごとに異なっておりますので、本ラボラトリーズパックのIP Lockコアを他のラボラトリーズパックの暗号処理チップと共に使用することはできません。IP Lock コアと暗号処理チップは必ず同じラボラトリーズパック内の組としてご使用ください。

[3] ユーザ専用の ID は各ラボラトリーズパック限りのものですので、ご購入されたラボラトリーズパックと同一 ID を持つ暗号処理チップの追加入手はできません。別IDを持つラボラトリーズパックをご購入ください。製品版搭載時のような大量のチップをご使用の場合のために、ユーザ任意の ID を書き込むことが可能な IP Lock ライタ(IPL-003WR)およびブランク暗号処チップ(IPL-CHP)をご用意しております。

[4] 暗号処理チップの基板への実装の際は取り付け方向にご注意ください。

[5] 暗号処理チップの基板への実装の際は静電気にご注意ください。静電気はデバイスを破損する恐れがあります。

[6] 暗号処理チップの電圧範囲は2.5あるいは3.3Vです。電源の誤使用によるモジュール破損は保証/交換の対象とはなりませんのでご注意ください。

[7] Altera 社製 FPGA をご使用する場合には別途弊社にライセンスファイルを申請する必要があります。登録に必要な事項を弊社IP Lockサポート(iplock@design-gateway.com)までメールにてお知らせください。

[個人情報の取り扱いについて]

お知らせ頂く情報はライセンスファイル発行の必要情報として厳重に管理されます。ほかの目的に利用されたり第三者に譲渡されることはありません。

システム概要

IP Lockコアはユーザ鍵(ID)を確認しながら暗号処理チップと通信します。IDと一致すればIP Lockコアはイネーブル信号(1)を出力します。一致しない場合はディセーブル(0)となります。このイネーブル信号をユーザロジックに対して出力させることにより、ID が一致するときのみユーザロジックを動作可能にさせることができます。 図 1 に IP Lock システムのブロック図を示します。FPGA と暗号処理チップは、DC0 および DD0 の 2 本の信号線で接続します。IP Lock コア自体の動作クロックとして、SC0 をユーザロジックより供給する必要があります。この SC0 の周波数は 1-25MHz の範囲となるクロックを供給してください。
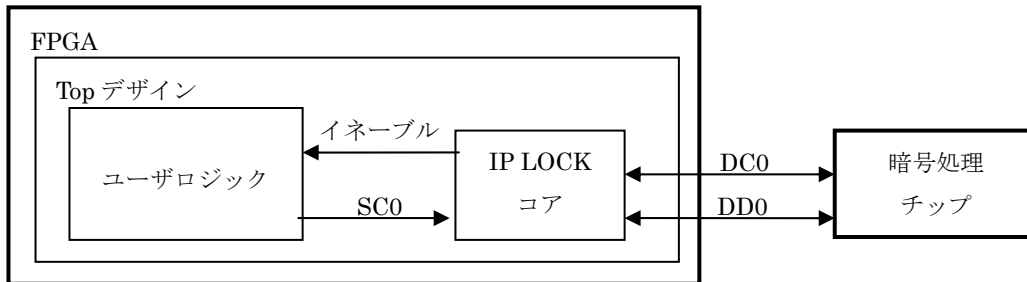
図 1 IP Lock システムブロック図

IP Lock コアからのイネーブル信号は SC0 に同期して出力されますが、ユーザロジック側のシステムクロックが SC0 と異なる場合、イネーブル信号を同期化する必要があります。この場合、下図2のようにDフリップフロップをユーザロジック内に追加し、必ずユーザクロックと同期させた後のイネーブル信号を使ってください。
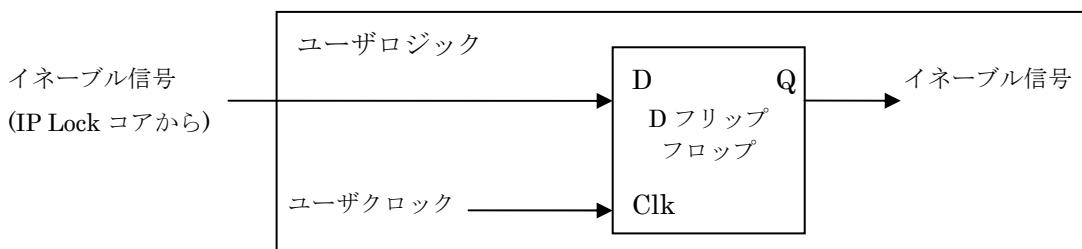
図 2 イネーブル信号の同期

IP Lock コア

図 3 に IP Lock コアのトップレベルのブロック図を示します。
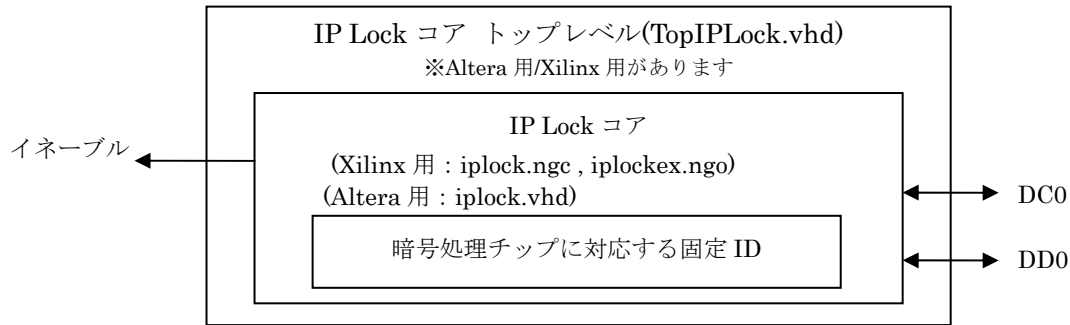
図 3　IP Lock コア　トップレベル

IP Lock コア(Xilinx 用:ipLock.ngc, ipLockex.ngo / Altera 用:iplock.vhd)は ID を確認するため暗号処理チップと通信します。ID が一致した時のみ、イネーブル信号を出力します。

■**Xilinx ユーザ**:

ipLock.ngc, ipLockex.ngo 両ファイルを Xilinx プロジェクトフォルダにコピーし、HDL コードを合成・インプリメントしてください。

■**Altera ユーザ**:

Altera 用 IP Lock コアは暗号化されているため HDL コードを合成・インプリメントする前に、IP Lock ライセンスを QuartusII ライセンスに追加する必要があります。

IP Lock のライセンスファイルは、弊社 IP Lock サポートにメールにて登録頂くことにより発行致します。登録に必要な事項を弊社 IP Lock サポート(iplock@design-gateway.com)までメールにてお知らせください。

Altera ユーザ用 IP Lock ライセンス取得の流れ:

1. デザイン・ゲートウェイ IP Lock サポートに下記情報をメールにて通知してください。
   宛先のメールアドレスは、iplock@design-gateway.com です。

氏名 : ....
会社名 : ....
IP Lock シリアル番号: (ケースおよび CD-ROM に記載)........
ボリュームシリアル番号 : ....
住所 : ....
Tel /Fax : ....

図 4　ライセンスファイル発行　登録事項

Windows のインストールされているドライブのボリュームシリアル番号をお知らせください。ボリュームシリアル番号は、DOS プロンプトの"dir"コマンドで知ることができます。表示方法を図 5 に示します。

```
C:¥>dir
ドライブ C のボリュームラベルがありません。
ボリューム シリアル番号は A035-6978 です

C:¥ のディレクトリ
2005/06/01210:33              0 AUTOEXEC.BAT
```

図 5　ボリュームシリアル番号の表示

2. デザイン・ゲートウェイは IP Lock ライセンスを発行し、2 営業日以内にお客様へメールにて返送します。
3. Quartus II のライセンスファイルをノートパッド等で開き、受け取った IP Lock ライセンスを図 6 のように追加してください。
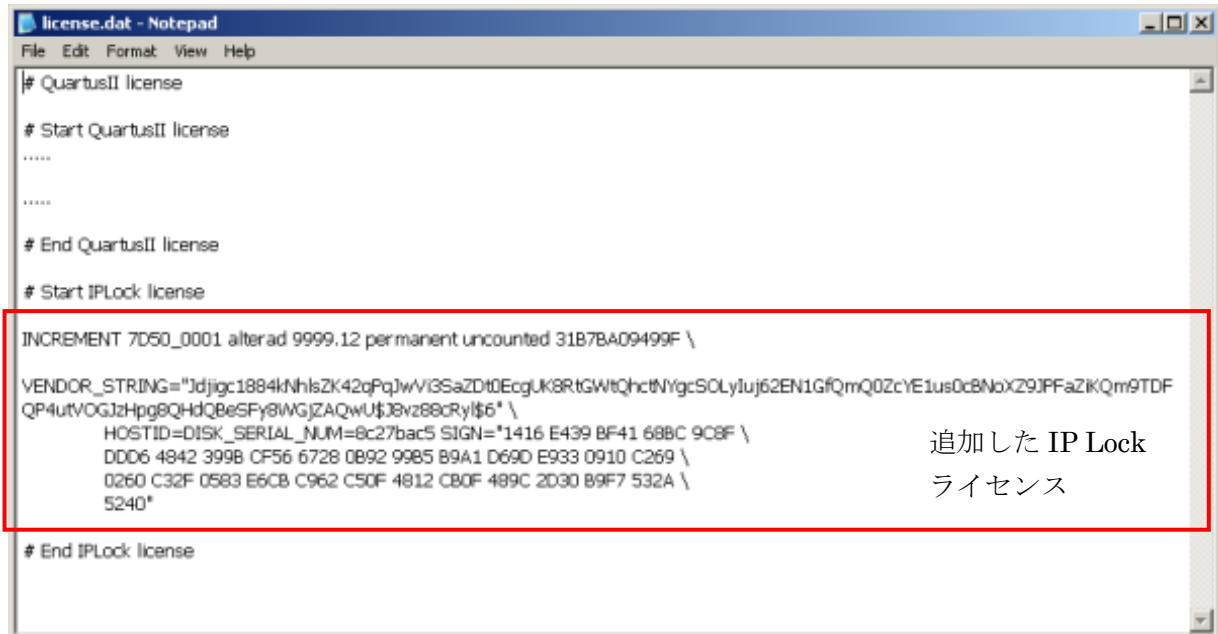
図 6　Quartus II ライセンス内に追加した IP Lock ライセンス(例)

暗号処理チップ回路図
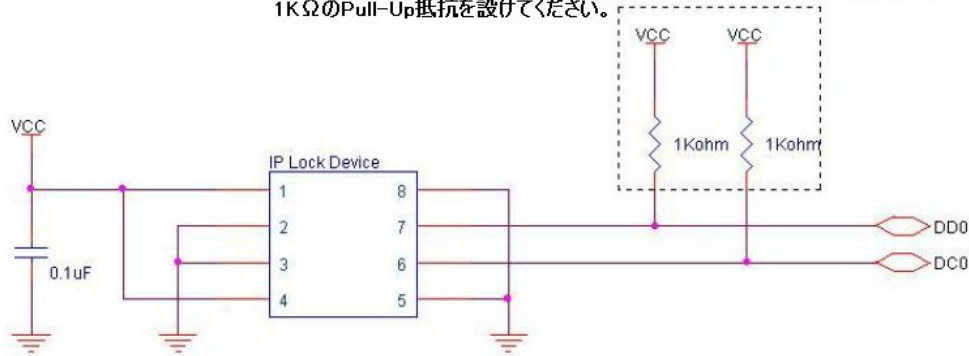
図 7　暗号処理チップ回路例

FPGA と暗号処理チップとの接続には DC0 および DD0 の 2 本の信号線を必要とします。図 7 に暗号処理チップの推奨回路図を示します。

DC0 および DD0 はプルアップし FPGA の I/O ピンと接続し、更に基板上に 1KΩの PullUp 抵抗を実装してください。FPGA の内蔵 Pull-Up 機能はインピーダンスが高く外来ノイズの影響による誤動作の恐れがありますので使わないでください。 暗号処理チップの適正電圧は 2.5V または 3.3V です。接続する FPGA の I/O ピンと同じレベルの電圧を印加してください。

暗号処理チップの 1,4 ピンは VCC に、2,3,5,8 ピンは GND に接続してください。

暗号処理チップ寸法、電気的特性

暗号処理チップは SOP8 ピンパッケージです。図 8 にパッケージの外形寸法を示します。
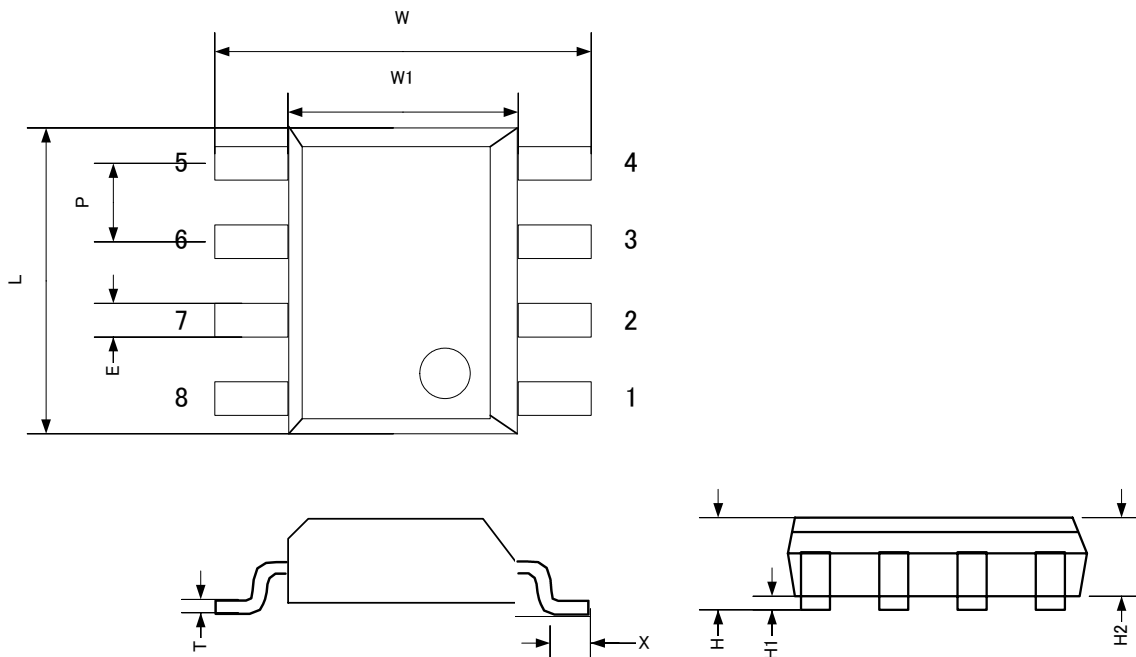
図 8　暗号処理チップ　パッケージ外形寸法図

表　暗号処理チップ　パッケージ各部寸法(単位:mm)

項目	記号	最小	平均	最大
実装時高さ	H	1.35	1.55	1.75
スタンドオフ	H1	0.10	0.18	0.25
パッケージ厚	H2	1.32	1.42	1.55
チップ全体幅	W	5.79	6.02	6.20
パッケージ幅	W1	3.70	3.91	4.00
パッケージ長さ	L	4.80	4.90	5.00
ピンのリード･ピッチ	P		1.27	
ピンのリード幅	E	0.33	0.42	0.51
ピンのリード厚	T	0.20	0.23	0.25
ピンのフット長	X	0.48	0.62	0.76

暗号処理チップの電気特性を下記に示します。

[絶対最大定格]
保存温度：　-40℃～+125℃
動作温度：　-20℃～+85℃
電圧範囲：　-0.3V～+3.3V

[推奨動作条件]
動作温度範囲：　0℃～+70℃
動作電圧範囲：　2.5V 動作時　2.25V～2.75V
3.3V 動作時　3.0V～3.6V

暗号処理チップパターン寸法

図 9 に暗号処理チップの推奨フットパターン寸法を示します。
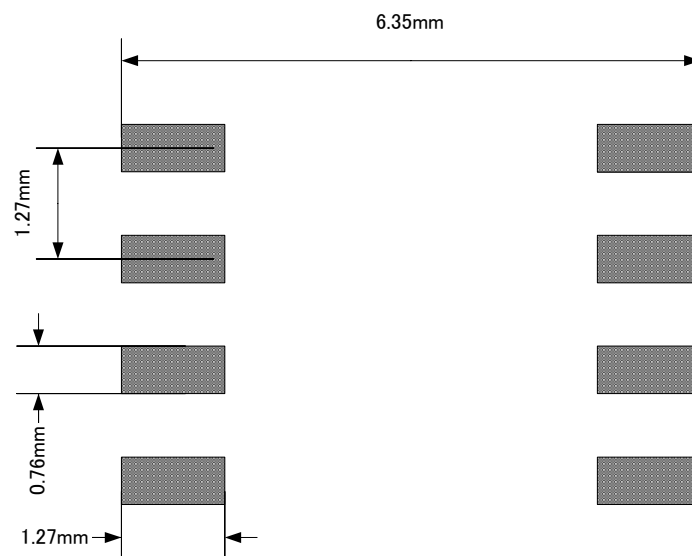
図 9　基板の推奨フットパターン寸法

VHDL デザイン例

CD-ROM には Counter.vhd と Counter32bits.vhd の 2 つのサンプルソースコードを収録しています。Counter.vhd は、ユーザロジックと IP LOCK コア トップレベル(TopIPLock.vhd)との接続方法を示すデザイン例です。Counter32bits.vhd は、IP Lock コアからのイネーブル信号をユーザロジックで使用するデザイン例です。図 10 に VHDL デザイン例のブロック図を示します。
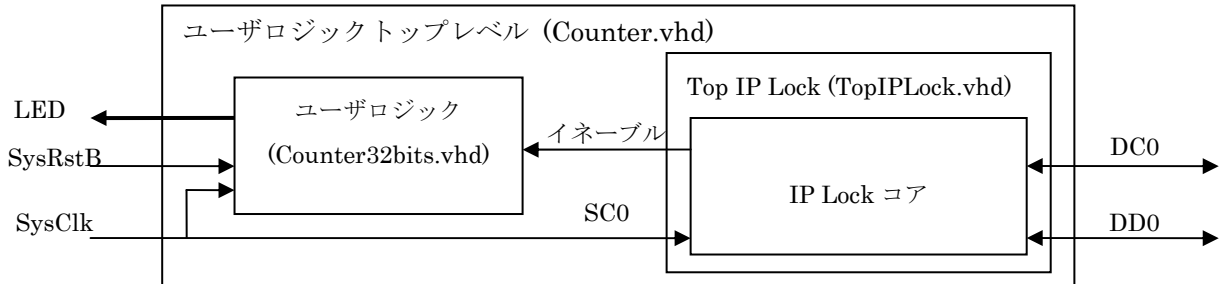
図 10 VHDL デザイン例 ブロック図

図 11、図 12 に VHDL デザイン例ソースファイルのインプリメントの方法を示します。

■Xilinx ユーザ:
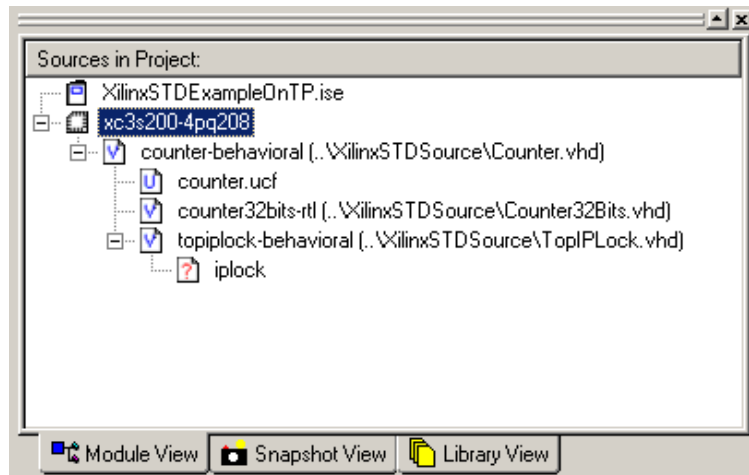
図 11 Xilinx ISE プロジェクトへのインプリメント例

■Altera ユーザ:
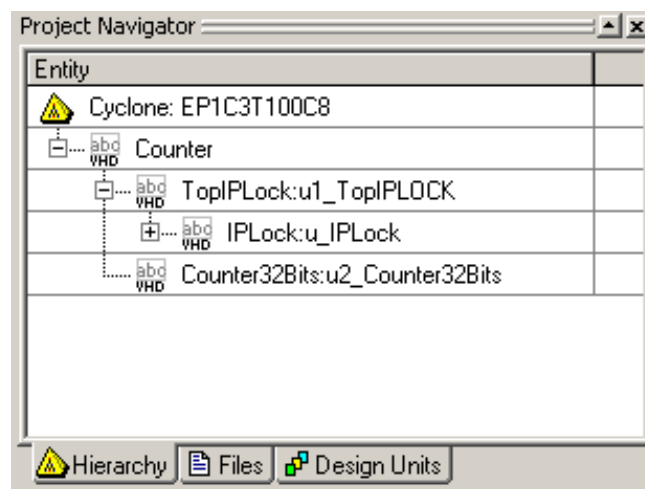
図 11 Quartus II プロジェクトへのインプリメント例

主な仕様

◆暗号方式:　AES-128 暗号方式
◆消費リソース:　約 400 スライス/2 ブロック RAM (Xilinx),
約 1200LE/約 24,500 メモリビット(Altera)
◆IP Lock 機能:　暗号処理チップと ID が一致したときのみイネーブル出力、不一致の場合ディセーブル、ユーザロジックの機能(一部あるいはすべて)が停止
約 200msec サイクルで認証データを変更・暗号化
◆対応デバイス:　**Xilinx**: Spartan-2, Spartan-2E, Spartan-3, Spartan-3E, Spartan-6
Virtex, Virtex-2, Virtex-2Pro, Virtex-4, Virtex-5, Virtex-6
Altera: Stratix, Stratix2, Stratix3, Stratix4, ArriaGX, Arria2GX
Cyclone, Cyclone2, Cyclone3
※2010 年 10 月現在。最新対応デバイスについては、弊社ホームページ IPLock-LIST.pdf をご確認下さい。
◆要求システム環境:　Xilinx ISE 7.1 以上の FPGA デザインツール、あるいは
Altera QuartusII 4.1 以上の FPGA デザインツール
◆オプション:　「IP Lock ライタ IPL-003WR」を使用することにより、ブランクの暗号処理チップ(IPL-CHP、別売)に任意の ID を書き込むことができます。

免責事項

IP Lock の使用により生じたユーザ回路基板および基板上のデバイスの損害については免責事項とさせていただきます。また、IP Lock を改造して使用した場合の品質保証は致し兼ねます。
第 3 者によって IP Lock のセキュリティ・システムが逆解析されたことで生じたお客様の損失については免責事項とさせていただきます。
IP Lock のセキュリティ強度につきましては、応用製品を市場に投入される前に、ラボラトリーズパックや評価ボード等で、お客様にて十分なご評価を行っていただく必要があります。

[問い合わせ先]
URL : http://www.dgway.com
Email : info@dgway.com

■ お問い合わせの前に ■

暗号処理チップを FPGA と接続、IP Lock コアとユーザ回路が正常にコンパイルされ、FPGA に正常にダウンロードされたことを確かめた後、IP Lock が動作しない場合、下記の点をご確認ください。

- 暗号処理チップは正しい方向にマウントされていますか? 本取扱説明書「図 8 暗号処理チップ回路例」を確認し、適切な方向にマウントしてください。
- FPGA 内のピンアサインは適正ですか?　本取扱説明書「図 8 暗号処理チップ回路例」を確認し、適切なピンアサインをしてください。
- 暗号処理チップに適正な電圧が印加されていますか？　接続する FPGA の I/O ピンと同じレベルの電圧を印加 してください。尚、暗号処理チップの適正電圧は 2.5 あるいは 3.3V です。
- 暗号処理チップの DD0 と DC0 はプルアップされていますか? またプルアップ抵抗値は 1KΩでしょうか？
- IP Lock コアと暗号処理チップは同一ラボラトリーズパック内のものですか？ ID は各ラボラトリーズパックのセットごとに異なっております。異なるパックの IP Lock コアと暗号処理チップを共に使用することはできません。
- 以上の点をご確認いただいても IP Lock が動作しない場合は弊社までお問い合わせください。